AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (currently amended) An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the decoy device comprises:

an attack detector for detecting presence or absence of an attack by receiving the input IP packet from the firewall device, and executing a network service process ~~for~~ responsive to the received input IP packet ~~transferred from the firewall device~~, and

the firewall device comprises:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the

header information of the input IP packet and a distribution condition; and

a filtering condition manager for managing the filtering condition depending on whether the attack detector detects an attack based on the input IP packet forwarded to the decoy device.

2. (original) The attack defending system according to claim 1, wherein the header information of an input IP packet includes at least one of a source IP address and a destination IP address thereof,

wherein the destination selector selects a destination of the input IP packet depending on whether the header information of the input IP packet satisfies the distribution condition.

3. (original) The attack defending system according to claim 1, wherein the destination selector comprises a memory for storing as the distribution condition a guiding list containing a set of IP addresses unused in the internal network, wherein the destination selector selects the decoy device when a destination IP address of the input IP packet matches an unused IP address contained in the guiding list.

4. (original) The attack defending system according to claim 1, wherein the destination selector comprises:

a packet buffer for storing input IP packets; and

a monitor for monitoring reception of a destination unreachable message after an input IP packet has been transferred from the packet buffer to the internal network,

wherein, when the monitor detects the reception of the destination unreachable message for the input IP packet, the input IP packet is transferred from the packet buffer to the decoy device.

5. (original) The attack defending system according to claim 1, wherein the firewall device further comprises:

a distribution condition updating section for updating the distribution condition depending on whether the attack detector detects an attack based on the input IP packet transferred to the decoy device.

6. (original) The attack defending system according to claim 1, wherein the filtering condition manager stores the filtering condition with a limited validity period, which corresponds to the header information of the input IP packet forwarded to the decoy device, wherein, when the limited validity period has elapsed, a default filtering condition is returned to the packet filter.

7. (original) The attack defending system according to claim 1, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

8. (original) The attack defending system according to claim 6, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

9. (original) The attack defending system according to claim 1, wherein the decoy device comprises:

an event memory for temporarily storing events related to at least network input/output, file input/output, and process creation/termination; and

an event manager for analyzing cause-effect relations of the events stored in the event memory to form links among the events.

10. (original) The attack defending system according to claim 1, wherein the attack detector detects an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

11. (original) The attack defending system according to claim 9, wherein the attack detector detects an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

12. (original) The attack defending system according to claim 11, wherein the attack detector searches the links to extract at least, a generation event of a process generating an event to be inspected and a network reception event by which the event to be inspected is generated, when determination is made based on the domain constraint and the type constraint.

13. (original) The attack defending system according to claim 1, further comprising a mirroring device for copying at least a file system from a server on the internal network to the decoy device, wherein when an attack is detected by the decoy device, the mirroring device copies at least the file system from the server on the internal network to the decoy device.

14-112. (canceled)

113. (new) An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the decoy device comprises:

an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device, and

the firewall device comprises:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution condition; and

a filtering condition manager for managing the filtering condition depending on whether the attack detector detects an attack based on the input IP packet forwarded to the decoy device, wherein

the destination selector comprises a memory for storing as the distribution condition a guiding list containing a set of IP addresses unused in the internal network, the destination selector selecting the decoy device when a destination IP address of the input IP packet matches an unused IP address contained in the guiding list.

114. (new) The attack defending system according to claim 113, wherein the firewall device further comprises:

a distribution condition updating section for updating the distribution condition depending on whether the attack detector detects an attack based on the input IP packet transferred to the decoy device.

115. (new) The attack defending system according to claim 113, wherein the filtering condition manager stores the

filtering condition with a limited validity period, which corresponds to the header information of the input IP packet forwarded to the decoy device, wherein, when the limited validity period has elapsed, a default filtering condition is returned to the packet filter.

116. (new) The attack defending system according to claim 115, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

117. (new) An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the decoy device comprises:

an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device, and

the firewall device comprises:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution condition; and

a filtering condition manager for managing the filtering condition depending on whether the attack detector detects an attack based on the input IP packet forwarded to the decoy device,

wherein the destination selector comprises:

a packet buffer for storing input IP packets; and

a monitor for monitoring reception of a destination unreachable message after an input IP packet has been transferred from the packet buffer to the internal network,

wherein, when the monitor detects the reception of the destination unreachable message for the input IP packet, the

input IP packet is transferred from the packet buffer to the decoy device.

118. (new) The attack defending system according to claim 117, wherein the firewall device further comprises:

a distribution condition updating section for updating the distribution condition depending on whether the attack detector detects an attack based on the input IP packet transferred to the decoy device.

119. (new) The attack defending system according to claim 117, wherein the filtering condition manager stores the filtering condition with a limited validity period, which corresponds to the header information of the input IP packet forwarded to the decoy device, wherein, when the limited validity period has elapsed, a default filtering condition is returned to the packet filter.

120. (new) The attack defending system according to claim 119, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

121. (new) An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the decoy device comprises:

an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device, and

the firewall device comprises:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution condition; and

a filtering condition manager for managing the filtering condition depending on whether the attack detector detects an attack based on the input IP packet forwarded to the decoy device,

wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

122. (new) The attack defending system according to claim 121, wherein the header information of an input IP packet includes at least one of a source IP address and a destination IP address thereof,

wherein the destination selector selects a destination of the input IP packet depending on whether the header information of the input IP packet satisfies the distribution condition.

123. (new) The attack defending system according to claim 121, wherein the firewall device further comprises:

a distribution condition updating section for updating the distribution condition depending on whether the attack detector detects an attack based on the input IP packet transferred to the decoy device.

124. (new) The attack defending system according to claim 121, wherein the filtering condition manager stores the filtering condition with a limited validity period, which corresponds to the header information of the input IP packet forwarded to the decoy device, wherein, when the limited validity period has elapsed, a default filtering condition is returned to the packet filter.

125. (new) The attack defending system according to claim 124, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

126. (new) An attack defending system provided at an interface between an internal network and an external network,

comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the decoy device comprises:

an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device,

an event memory for temporarily storing events related to at least network input/output, file input/output, and process creation/termination, and

an event manager for analyzing cause-effect relations of the events stored in the event memory to form links among the events; and

the firewall device comprises:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution condition; and

a filtering condition manager for managing the filtering condition depending on whether the attack detector detects an attack based on the input IP packet forwarded to the decoy device.

127. (new) The attack defending system according to claim 126, wherein the header information of an input IP packet includes at least one of a source IP address and a destination IP address thereof,

wherein the destination selector selects a destination of the input IP packet depending on whether the header information of the input IP packet satisfies the distribution condition.

128. (new) The attack defending system according to claim 126, wherein the firewall device further comprises:

a distribution condition updating section for updating the distribution condition depending on whether the attack detector detects an attack based on the input IP packet transferred to the decoy device.

129. (new) The attack defending system according to claim 126, wherein the filtering condition manager stores the filtering condition with a limited validity period, which corresponds to the header information of the input IP packet

forwarded to the decoy device, wherein, when the limited validity period has elapsed, a default filtering condition is returned to the packet filter.

130. (new) The attack defending system according to claim 129, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

131. (new) The attack defending system according to claim 126, wherein the attack detector detects an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

132. (new) The attack defending system according to claim 131, wherein the attack detector searches the links to extract at least, a generation event of a process generating an event to be inspected and a network reception event by which the

event to be inspected is generated, when determination is made based on the domain constraint and the type constraint.

133. (new) An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the decoy device comprises:

an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device, and

the firewall device comprises:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution condition; and

a filtering condition manager for managing the filtering condition depending on whether the attack detector

detects an attack based on the input IP packet forwarded to the decoy device,

wherein the attack detector detects an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

134. (new) The attack defending system according to claim 133, wherein the header information of an input IP packet includes at least one of a source IP address and a destination IP address thereof,

wherein the destination selector selects a destination of the input IP packet depending on whether the header information of the input IP packet satisfies the distribution condition.

135. (new) The attack defending system according to claim 133, wherein the firewall device further comprises:

a distribution condition updating section for updating the distribution condition depending on whether the attack detector detects an attack based on the input IP packet transferred to the decoy device.

136. (new) The attack defending system according to claim 133, wherein the filtering condition manager stores the

filtering condition with a limited validity period, which corresponds to the header information of the input IP packet forwarded to the decoy device, wherein, when the limited validity period has elapsed, a default filtering condition is returned to the packet filter.

137. (new) The attack defending system according to claim 136, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

138. (new) An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the decoy device comprises:

an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device, and

the firewall device comprises:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution condition;

a filtering condition manager for managing the filtering condition depending on whether the attack detector detects an attack based on the input IP packet forwarded to the decoy device; and

a mirroring device for copying at least a file system from a server on the internal network to the decoy device, wherein when an attack is detected by the decoy device, the mirroring device copies at least the file system from the server on the internal network to the decoy device.

139. (new) The attack defending system according to claim 138, wherein the header information of an input IP packet

includes at least one of a source IP address and a destination IP address thereof,

wherein the destination selector selects a destination of the input IP packet depending on whether the header information of the input IP packet satisfies the distribution condition.

140. (new) The attack defending system according to claim 138, wherein the firewall device further comprises:

a distribution condition updating section for updating the distribution condition depending on whether the attack detector detects an attack based on the input IP packet transferred to the decoy device.

141. (new) The attack defending system according to claim 138, wherein the filtering condition manager stores the filtering condition with a limited validity period, which corresponds to the header information of the input IP packet forwarded to the decoy device, wherein, when the limited validity period has elapsed, a default filtering condition is returned to the packet filter.

142. (new) The attack defending system according to claim 141, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

143. (new) An attack defending system provided at an interface between an internal network and an external network, the system comprising:

a firewall device, having a packet filter, a destination selector, and a filtering condition manager; and

a decoy device, having an attack detector, connected to the firewall device,

the packet filter configured to determine whether an input IP packet inputted from an external network is to be accepted for passing to the destination selector, the determination based on header information of the input IP packet and a filtering condition as set by the filter condition manager,

the destination selector receiving the input IP packet from the packet filter and configured to select one of an internal network and the decoy device as a destination for the input IP packet accepted by the packet filter, the selection

based on the header information of the input IP packet and a distribution condition,

the decoy device configured to receive the input IP packet from the destination selector and execute a network service process responsive to the received input IP packet,

the attack detector configured to detect an attack on the decoy device resulting from the received input IP packet and provide a detection status, and

the filtering condition manager configured to manage the filtering condition of the packet filter based on the detection status provided by the attack detector, so that the filtering condition for a subsequently received input IP packet is upgraded upon a positive detection status being provided by the attack detector.